IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No.: 8159
Satyajit NATH	Art Unit: 2432
Appl. No.: 10/815,251	Examiner: Kim, Jung W.
Filed: March 30, 2004	Atty. Docket: 2222.5500000
For: **Method and System for Providing Document Retention Using Cryptography**	

DRAFT

Proposed Claim Amendments to be discussed during telephonic interview

PROPOSED CLAIMS--FOR DISCUSSION PURPOSES ONLY--NOT TO BE ENTERED INTO FORMAL RECORD

Proposed Amendments to the Claims

Support for the proposed amendments is found at least at, for example, paragraphs [0014], [0020], and [0098] - [0043] and FIGs. 1 and 5-11 and originally filed claim 38 of Publication No. 2005/0223242 A1 to Satyajit NATH (alternatively, "the Specification.").

Amendments to the Claims

29. (Proposed amended) A computer-implemented method for distributing cryptographic keys used in a file security system, said method comprising:

receiving, at a computing device, a request for a document retention key that is necessary to gain access to a cryptographically secured electronic document;

identifying, by the computing device, a document retention period associated with the document retention key, the document retention period being dependent on a future event that was unscheduled when the document retention period was associated with the electronic document;

determining, by the computing device, whether the document retention period associated with the document retention key has been exceeded; and

refusing to distribute the document retention key in response to determining that the document retention period for the electronic document has been exceeded.

30. (Proposed amended) The computer-implemented method as recited in claim 29, wherein the document retention period is a predetermined period of time after the occurrence of the future event.

31. (Proposed amended) The computer-implemented method as recited in claim 29, wherein said computing device is ~~method is performed at~~ a server, and wherein the request for the document retention key is from a client module that is connectable to the server via a network.

32. (Proposed amended) The computer-implemented method as recited in claim 29, wherein the document retention period can be extended to permit extended access to the electronic document.

33. (Proposed amended) A file security system ~~for restricting access to electronic files, said file security system~~ comprising:

a processor;

a memory having instructions stored thereon, that, in response to execution by the processor, cause the processor to restrict access to electronic files, the instructions comprising:

instructions for storing ~~a key store that stores~~ a plurality of cryptographic key pairs in a key store, each of the cryptographic key pairs including a public key and a private key, at least one of the cryptographic key pairs pertaining to a retention policy, the retention policy being dependent on a future event; and

instructions for determining ~~an access manager operatively connected to said key store, said access manager determines~~ whether the private key of the at least one of the cryptographic key pairs pertaining to the retention policy is permitted to be provided to a requestor based on whether the future event has occurred,

wherein the requestor requires the private key of the at least one of the cryptographic key pairs pertaining to the retention policy to access a secured electronic file, and wherein the secured electronic file was previously secured using the public key of the at least one of the cryptographic key pairs pertaining to the retention policy, and at the time the electronic file was so secured, the future event was unscheduled.

34. (Proposed amended) The file security system as recited in claim 33, wherein ~~said access manager prevents~~ the instructions for determining comprise instructions for preventing the private key of the at least one of the cryptographic key pairs pertaining to the predetermined time from being provided to the requestor after a predetermined retention period following the occurrence of the future event.

38. (Proposed amended) A ~~tangible~~ non-transitory computer readable medium having instructions stored thereon for providing data retention for electronic data, the instructions comprising:

instructions to assign a data retention policy to the electronic data, the data retention policy being based on a future event that is unscheduled; and

instructions to cryptographically associate, using a cryptographic key, the data retention policy with the electronic data.